REMARKS/ARGUMENTS

In response to the Office Action of June 8, 2005, please consider the following remarks.

Claims 1-76 are currently pending in the application.

In the Office Action mailed June 8, 2005, claims 1, 3, 4, 9, 11, 12, 17, 19, 20, 25, 27, 28, 32, 34-36, 38, 39, 46, 48, 49, 52, 54-56, 58-60, 64, 66, 68, 69, and 71-76 were rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. Claims 1, 5-9, 13-17, 21-25, 29-32, 46, 50-52, 56, 60-63, 75, and 76 were rejected under 35 U.S.C. § 102(b) as being anticipated by US Patent 4,964,164 (hereinafter, "Fiat"). Claims 2, 10, 18, 26, 33, 36, 37, 40-45, 47, 53, 57, 64-67, and 70-74 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Fiat in view of US Patent 6,763,459 (hereinafter "Corella"). Claims 3, 4, 11, 12, 19, 20, 27, 28, 34, 35, 38, 39, 48, 49, 54, 55, 58, 59, 68, and 69 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Fiat in view of Corella, and further in view of US Patent 6,757,823 (hereinafter "Rao et al.").

Reconsideration of the instant application by the Examiner in view of the remarks below is respectfully requested.

Contrary to the Examiner's assertion at page 5 of the Office Action, the applicants do not agree with the Examiner that Fiat, Corella, and Rao et al. disclose "a computation method for batch processing of public key encryption using a processor and a registration authority that issues a first unsigned certificate that binds a public key of the subject to long term identification information related to the subject and maintains a certificate database." These and other assertions of the Examiner are discussed below.

The 112 Rejections

The Applicants have amended claims 1, 9, 17, 25, 32, 36, 46, 52, 56, 60, 64, 66, and 71-76 to claim batch processing that includes any size batch (as opposed to a batch of size four). The applicants respectfully point out that a batch size of four is covered by the claims as amended. The applicants reserve the right to reintroduce claims that include a batch size of four.

The Applicants have amended the specification to include a paragraph [0126.1] that includes language from claims 3, 4, and 5. Since the material was inherently contained in the original application (i.e., in claims 3, 4, and 5), no new matter has been added.

The Prior Art (102 Rejections)

Fiat explains at Col. 3, lines 34-38 that "a modification to the RSA method that allows far more efficient processing when the digital signatures are to be generated in a batch mode. That is, when several digital signatures are to be generated at once." Notably, Fiat does not describe combining encrypted messages. Rather, Fiat describes techniques for generating digital signatures at once, which is characterized in the Fiat reference as "batch mode".

At Col. 2, lines 63-66, Fiat explains that "[a]nother object of the present invention is to provide a method for efficiently transforming enciphered-message-data signals and generating signed-message-data signals in a batch mode." At Col. 3, lines 45-55, Fiat explains that "[w]hen using the RSA scheme for several documents needing the identical signature, one must activate the scheme for each and every signature, so that a person wishing to use the scheme for several documents, or a central computer having to analyze many signatures, will have to use up long and expensive computer time. The present invention provides a method for using the RSA scheme for simultaneously signing in parallel, or analyzing in parallel ***the same signature***, by

using the exponential formula one time" (emphasis added). Thus, the "batch" describes a batch of related signals.

The Prior Art Distinguished (102 Rejections)

Claim 1 includes the language "combining individually encrypted network security protection handshake messages into a set of encrypted messages wherein each encrypted handshake message is derived using a public key containing an encryption exponent[.]" Fiat does not disclose combining individually encrypted messages or combining handshake messages. The Examiner asserted at page 7 of the Office Action that this is taught by Fiat at Col. 1, line 25 to Col. 2, line 57; Col. 3, line 63 to Col. 4, line 43; and at Col. 5, lines 20-56. However, the Applicants have carefully read the cited passages and have found no such teaching. Indeed, since Fiat describes signing in parallel, or analyzing in parallel the same signature, the Applicants respectfully submit that Fiat would have no obvious reason to combine individually encrypted messages, or handshake messages.

Claim 1 includes the language "determining a root node of a binary tree comprising leaf nodes corresponding to each encryption exponent[.]" Fiat does not disclose a binary tree, much less a root node of a binary tree. The Examiner asserted at page 7 of the Office Action that this is taught by Fiat at Col. 3, line 63 to Col. 4, line 43 and Col. 5, lines 20-50. However, the Applicants have carefully read the cited passages and have found no such teaching. Indeed, it is not clear how Fiat would use a binary tree with leaf nodes corresponding to each encryption exponent.

Claim 1 includes the language "decrypting the encrypted messages by expressing the at least one root as at least one promise and evaluating the at least one promise at the leaf nodes decreasing the number of modular inversions wherein efficiency of the decryption is increased." The Examiner asserted at page 7-8 of the Office Action that this is taught by Fiat at Col. 1, line 63 to Col. 2, line 11 and Col. 6, line 53 to Col. 7, line 4. However, the Applicants have carefully read the cited

passages and have found no such teaching. Fiat does not even disclose batch mode decryption (only encryption). Moreover, it is not clear how Fiat could evaluate a promise "at the leaf nodes" since no binary tree is used. Furthermore, Fiat does not describe decreasing the number of modular inversions wherein efficiency of the decryption is increased.

To anticipate a claim, a prior art reference must teach each and every element of the claim. Since Fiat does not teach each and every element of Claim 1, Claim 1 is allowable over Fiat. Independent Claims 9, 17, 25, 32, 46, 52, 56, 75, and 76 are at least allowable for reasons similar to those described above with reference to Claim 1. It may be noted that Claim 46 and 56 include the language "batch decryption in a computer network", and Fiat does not disclose batch decryption. Dependent claims 2-8, 10-16, 18-24, 26-31, 33-35, 47-51, 53-55, and 57-63 are allowable at least for depending from an allowable base claim.

The Prior Art (103 Rejections)

Fiat has been described above. Corella does not teach, and the Examiner did not assert that Corella teaches, batch decryption. Rao is used only to reject dependent claims, which are believed to be allowable at least for the reasons given below.

The Prior Art Distinguished (103 Rejections)

Claim 36 includes the language "batching handshake messages on a batch-decryption server according to the public key such that the disparity between the sizes of the encryption exponents of the public key is minimized[.]" Fiat does not disclose a batch-decryption server, or batching according to a public key such that the disparity between sizes of the encryption exponents of the public key is minimized. The Examiner asserted at page 22 of the Office Action that this is taught by Fiat at Col. 1, line 25 to Col. 2, line 57; Col. 3, line 63 to Col. 4, line 43; and at Col. 5, lines 20-56. However, the Applicants have carefully read the cited passages and have found no

such teaching. Fiat does not disclose batch-decryption at all. And Fiat does not batch according to the public key.

Claim 36 includes the language "separating the batch's e^{th} root in a downward percolation phase into constituent decrypted messages, wherein internal inversions are converted to modular divisions increasing efficiency by producing a reduced number of modular inversions[.]" Fiat does not separate the batch's e^{th} root in a downward percolation phase into constituent decrypted messages. The Examiner asserted at page 22 of the Office Action that this is taught by Fiat at Col. 4, lines 12-58 and Col. 5, lines 20-56. However, the Applicants have carefully read the cited passages and have found no such teaching.

Claim 36 includes the language "scheduling the batch decryption server based on server load considerations[.]" Claim 36 includes the language "decrypting the handshake messages using at least one alternate expression of at least on arithmetic function of at least one batch's e^{th} root[.]" Claim 36 includes the language "sending the decrypted message to the web server." These elements are not found in the Fiat reference.

The Applicants respectfully assert that Corella does not teach, and the Examiner did not suggest that Corella teaches, the above-identified elements of Claim 36. Since Fiat and Corella, whether considered alone or in combination, do not teach each and every element of Claim 36, Claim 36 is allowable over the references. Independent Claims 64, 66, and 71-74 are at least allowable for reasons similar to those described above with reference to Claim 36 and/or for reasons similar to those described above with reference to the 102 rejections. Dependent claims 37-45, 65, and 67-70 are allowable at least for depending from an allowable base claim.

Conclusion

In view of the foregoing, the Applicants respectfully submit that the pending claims are allowable. The Applicants respectfully request the Examiner withdraw the

rejections of all claims. The Applicants respectfully request that a timely Notice of Allowance be issued in this case.

Should the Examiner have any questions or comments, he is encouraged to call the undersigned at (650) 838-4305 so that any outstanding issues can be expeditiously resolved.

Respectfully submitted,
Perkins Coie LLP

Date: October 6, 2005

William F. Ahmann
Reg. No. 52,548

Correspondence Address:
Customer No. 22918
Perkins Coie LLP
P.O. Box 2168
Menlo Park, California 94026
(650) 838-4300